documents which permit the user to use the new device with the same functionalities of the existing devices.

REMARKS

The present response is intended to be fully responsive to all points of objection and/or rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Applicants assert that the present invention is new, non-obvious and useful. Prompt consideration and allowance of the claims is respectfully requested.

Status of Claims

Claims 1 through 13 have been canceled.

claims 14 through 28 are on file.

Claims 14, 22 are Currently Amended.

CLAIM REJECTIONS

35 U.S.C. § 102 Rejections

Further to the examiner response in the office action dated December 09, 2008, the applicant has decided, for clarity reasons, and to avoid all examiner rejections, to amend independent claims 14 and 22 accordingly and as listed above.

The objective of the amended claims is to further recite the limitation that the new device obtains the same functionality of existing devices without the need of intervention of a third trusted authority and/or device, ay all stages of the method. An example for such functionality is a new smart card that obtains the functionality of an existing credit card, to be used for purchasing purposes without the need to approach the credit card company.

Therefore, independent claims 14 and 22 were amended.

All remaining claims on file, depend on claims 14 and 22 and therefore should be allowed as well.

Lee et al. (US Patent 6950941) discloses a system which enables secure registration of portable devices and/or personal computer (described as "LCM") for the secure transfer of digital content. The registration process described by **Lee** is comprised of the following phases: Firstly enabling functionality of the "LCM" comprising of : Authentication of a trusted authority ("ISP") by the "LCM" (Col. 8 ln 64 – Col. 9 ln 2); Establishing a secure connection between the "LCM" and "ISP" (Col.9 ln 3-7); Afterwards enabling a portable device ("PD") comprising of : the PD requests the LCM to register (Col.9 ln 10 – 11); transferring **to the ISP** and only through the "LCM" the PD certificate data (Col. 9 ln 12 – 16, "*...tosses the certificate data for its ID of manufacturer key to the LCM. The LCM* ***send them to its connected ISP***..."). Only after the ISP (obviously a trusted entity) authenticates the PD, a token is sent to the device through the LCM.

Independent claims 14 and 22 clearly recite the limitation of transferring functionalities of existing user's device into a new device without the intervention of a third trusted device. For further clarity, independent claims 14 and 22 are amended to explicitly recite the limitation at the different stages of the claimed method, i.e. when reading from the existing device into the new device the said certified digital document associated with the said user, without intervention of a third trusted authority and/or device; and generating by the new device a new certified digital document according to the said issuing policy of the said CA without intervention of a third trusted authority and/or device, when the new certified digital document permits the user to use the new device with the same functionality of the existing device.

The limitation of transferring functionalities of existing user's device into a new device without the intervention of a third trusted authority or device is not suggested, taught or disclosed by **Lee** or any other known prior art. As well established under U.S. patent law, for a reference to anticipate a claim, the reference must teach all elements of the claim.

In view of this response, the pending claims are deemed to be allowable. Their favorable reconsideration and allowance is respectfully requested.

Respectfully submitted,

E. Barkan

Elad Barkan
12 Habanin Street,
Kefar Sirkin 49935,
ISRAEL
Email: moti@barkan.org

Listing of Claims on file

1. **[Cancelled]** A secure method for generating digital documents that are certified by a known authority, comprising the steps of:

A. Programming an electronic device with a document issuing method that originates with the known authority, wherein the device further includes means for protecting the programmed method from tampering with;

B. programming the electronic device with data identifying the owner of the device, and wherein the device includes means to prevent subsequent alterations of the owner identification data;

C. reading a digital document into the device;

D. physical identification of the owner of the device, based on the identifying data as programmed in step (B);

E. if the result of the identification process in step (D) is positive, this indicating that the true owner requested the document, then issuing of a digital document signed by the known authority, wherein the document is prepared according to the document issuing method that was programmed into the device in step A.

2. **[Cancelled]** The secure method of claim 1, wherein in step A the programming further includes information that is unique to each device.

3. **[Cancelled]** The secure method of claim 1, wherein in step B the device reads a prior issued digital document that attests to a prior identification of the user, and wherein the information in that document is used for programming the electronic device with data identifying the owner of the device.

4. **[Cancelled]** The secure method of claim 1, wherein in step C the device reads a digital document relating to the owner of the device, and further including the step of verifying whether the identifying information in the document corresponds to the owner identification data entered in step B; proceeding to step D only if the identification result is positive, otherwise End procedure.

5. **[Cancelled]** The secure method of claim 1, wherein in step C the device reads a digital document sent to the owner of the device, and further including the step of verifying whether the addressee identity information in the document corresponds to the owner identification data entered in step B; proceeding to step D only if the identification result is positive, otherwise End procedure.

6. **[Cancelled]** The secure method of claim 1, wherein in step E the issued digital document is output through a communication channel in the device.

7. **[Cancelled]** The secure method of claim 1, wherein in step E the issued digital document is stored in digital storage means in the device.

8. **[Cancelled]** The secure method of claim 1, wherein in step E the issued digital document is a permit or a certificate.

9. **[Cancelled]** A device for generating digital documents that are certified by a known authority, comprising:

A. computer means with processing means and memory means for implementing a program written in the memory, and wherein the memory includes a document issuing method that originates with the known authority and data identifying the owner of the device;

B. means for protecting the document issuing method from tampering with;

C. means for preventing subsequent alteration of the owner identifing data;

D. input means for reading information related to physical user identification; and

E. output means for transmitting digital documents generated in the computer means.

10. **[Cancelled]** The device of claim 9, further including means for storing a plurality of digital documents and for retrieving any document as desired.

11. **[Cancelled]** The device of claim 9, further including an input/output channel for receiving documents or user's commands and for outputting digital documents as desired.

12. **[Cancelled]** The device of claim 9, wherein the device is stored in a wristwatch.

13. **[Cancelled]** The device of claim 9, wherein the device is stored in a smart device.

14. **[Currently Amended]** A method of transferring the functionality of a smart device ("existing device") to a different smart device ("new device"), without the need of intervention of a third trusted authority and/or device, whereas the said functionality of the existing device is allowed to the user by a certified digital document of a certifying authority (CA), comprising:

implementing in the new device a document issuing policy of the certifying authority (CA); and

reading from the existing device into the new device without the intervention of a third trusted device the said certified digital document associated with the said user; and

generating by the new device a new certified digital document according to the said issuing policy of the said CA, which permits the user to use the new device with the same functionality of the existing device.

15. **[Previously Amended]** The method according to claim 14, wherein information associated with the identity of the new device or it's user is stored within the new device.

16. **[Previously Amended]** The method of claim 14, wherein the issuing policy attests to personal identifying information of the user of the device.

17. **[Previously Amended]** The method of claim 14, wherein the new certified digital document is output by the new device through a communication channel.

18. **[Previously Amended]** The method of claim 14, wherein the certified digital documents are permits or certificates.

19. **[Previously Amended]** The method of claim 14, wherein a person using the new device to sign or certify a digital document is requested to identify himself prior to the new device signing or certifying the digital document.

20. **[Previously Amended]** The method of claim 19, wherein a user identifies himself using biometric identification information.

21. **[Previously Amended]** The method of claim 14, wherein a plurality of certified digital documents associated with the user are stored within the

new device, each of which plurality of certified digital documents is associated with a different certifying authority.

22. **[Currently Amended]** A smart device associated with a user, adapted to obtain the functionalities of the said user smart devices ("existing devices") , without the need of intervention of a third trusted authority and/or device, where the said functionalities are allowed by certified digital documents of a certifying authority (CA) comprising:

a controller adapted to execute a program associated with the certifying authority (CA) based on a document issuing policy of the certifying authority (CA); and

The controller reads a certified digital document associated with its user from the existing devices, and

According to the said issuing policy the controller generates, without intervention of a third trusted authority and/or device, a new certified digital documents which permit the user to use the new device with the same functionalities of the existing devices.

23. **[Previously Amended]** The smart device according to claim 22, wherein the said program generates the new certified digital document from a certified document associated with the user if data in the certified document is consistent with the document issuing policy.

24. **[Previously Amended]** The smart device of claim 22, wherein the controller reads a digital document provided to the smart device and signs or certifies the digital document only after the electronic device attests to personal identifying of the user.

25. **[Previously Amended]** The smart device of claim 24, further comprising a biometric data input module.

26. **[Previously Amended]** The smart device of claim 22, wherein a plurality of certified documents associated with the user are stored within the smart device, each of the plurality of certified documents are associated with a different certifying authority.

27. **[Previously Amended]** The smart device of claim 22, wherein the smart device is functionally associated with a wristwatch.

28. **[Previously Amended]** The smart device of claim 22, wherein the smart device is functionally associated with a smart card.